SSRG International Journal of Electronics and Communication Engineering
ISSN: 2348-8549/ https://doi.org/10.14445/23488549/IJECE-V11I12P121

Volume 11 Issue 12, 230-237, December 2024

Original Article

Blockchain Based Cryptographic Protocols for Secure Data Transmission

S. Senthil kumar[1], S. Rajaprakash[2], R. Jaichandran[3]

[1]*Department of Computer Science, School of Arts and Science, AV Chennai Campus, Vinayaka Missions Research Foundation (DU), Chennai, Tamil Nadu, India*
[2]*Department of Computer Science & Engineering, Vel Tech Rangarajan Dr.Sagunthala R&D Institute of Science and Technology, Chennai, Tamilnadu, India*
[3]*Aarupadai Veedu Institute of Technology, Vinakaya Mission's Research Foundation(Deeemed to be University), Tamil Nadu, India.*

[1]*Corresponding Author : 81senthil@gmail.com*

Received: 26 October 2024 Revised: 30 November 2024 Accepted: 14 December 2024 Published: 30 December 2024

Abstract *- The concept of blockchain is now gaining more and more attention than it did in the past. This technique provides an exceptionally high level of security to its potential users. Users are not very knowledgeable about the many ways in which the security of blockchain may be used to ensure the safety of the data that is sent. It has been hypothesised that the individual in question continued to use the "Salsa," a compact and secure device. The brand-new safety feature given the designation RPBB-24-6 is discussed in this academic work. An RPBB-24-6 encryption and decryption process is the way that has been offered, and this method comes with four different processes. Developing a covert message is the first step in the procedure. In the second step of the procedure, you will apply the secret code to each letter of the first secret message and then multiply the code by four times for each letter. Using the matrix as the third procedure, the encrypted data are applied. The application of the salsa approach constitutes the fourth step. Eventually, the plain text was transformed into data that was well secured.*

Keywords *- Decryption, Encryption, Performance, RPBB-24-6, Salsa.*

1. Introduction

Over the last several years, blockchain technology has entered almost every industry. The most important reason is that it utilises a novel and effective method for storing and transmitting data in a safe and traceable way. More data must be handled and stored safely as smart environments proliferate. The blockchain is assisting in protecting users' data and the anonymity of network participants. Blockchain technology is the most effective ledger for the transportation and storage of data, and a growing number of businesses all over the globe are embracing it as a result of its vast use in various industries, including finance, health care, and industry and logistics. Additionally, congestion, data loss, theft, and cost inflation are all reduced by using blockchain technology.

Ethereum is a layer-based blockchain. Figure 1 shows that the infrastructure layer controls node storage and encapsulates time-stamped data blocks. Hashing is among the many security constraints and consensus procedures in the platform and distributed computing layers. The platform layer is comprised of the Web API.

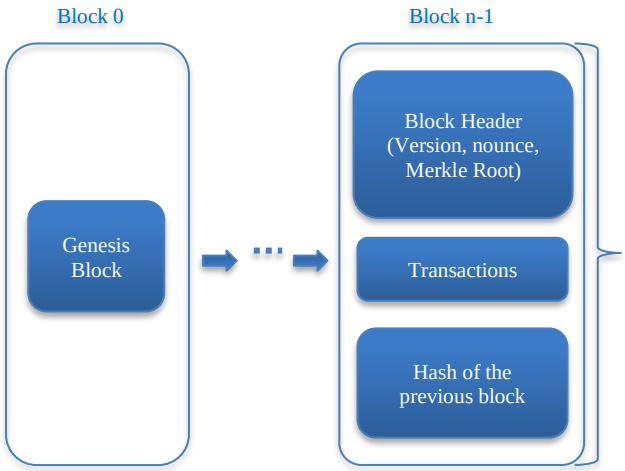

Fig. 1 The architecture of the blockchain

The application layer, which comprises commercial apps built on blockchain technology, is responsible for providing programmability to the blockchain. Blockchain technology assures the integrity and dependability of data in smart settings despite the vast volume of data that is being stored.

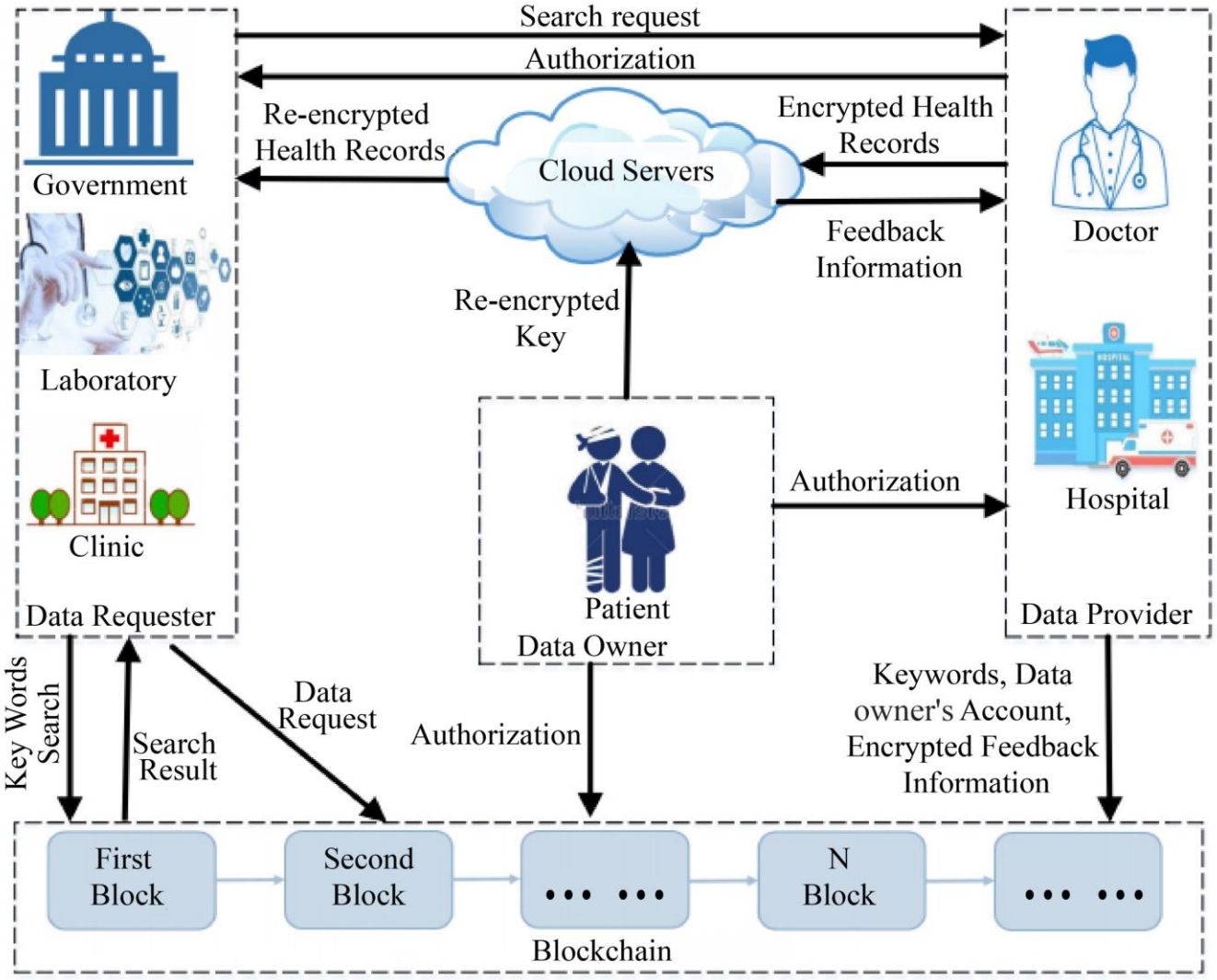

Fig. 2 The blockchain model of the system

The complexity of a distributed architecture that includes many devices and apps may be managed using blockchain technology. To be more precise, blockchain technology is now being recognised as an essential component for the management of Metaverse transactions. The purpose of smart settings is to make it easier for users to access services. Examples of some of the most frequent smart environment applications are shown in this area. Some examples include smart healthcare, transportation, and manufacturing.

From Figure 2, date owners are people who go to hospitals or other medical facilities to see doctors for medical care. After they talk, electronic health records with private information about each person will be made. Since DO is the source of the health records, they own and can change the data. They must create an account to share data on the EHR group blockchain. After getting the DO's OK, the DP can upload the health record to the cloud. People who want to view the info need to get permission from DO. Data producers are people like doctors and hospital managers who are in charge of EHRs. Once they get permission from the patient, they secure the health record and send the files to a cloud server. The cloud service is in charge of keeping the private EHR that DP sends. Its other job is to send the file's address to the DO's account in the EHR group blockchain. Data requesters are groups like the government, labs, clinics, and others that need to see a patient's EHR. First, they have to get the search trapdoor from DP and look for keywords in the blockchain. Once they find something, they have to send a request to DO. The re-encrypted health record will be sent to them from the cloud computer once they get permission from the DO. As shown in Figure 2, their work will create service transactions that will be added to the transaction pool. This means that they send service transactions in the blockchain. Like other users, they can join or leave the blockchain network anytime. In addition to using the system, they can see the whole agreement process.

2. Literature Survey

The author brought up several issues with blockchain technology. Its purpose is to evaluate the state of security [1]. [2] The topics of criminal assaults and crime prevention were explored. In order to evaluate the various degrees of security, the author investigated the content and structure of the blockchain [3]. They examined several potential dangers of developing double spending and Sybil, the two primary security approaches. This approach was used in the implementation of the security [4]. Additionally, S. Rajaprakash and his colleagues developed the more secure "RBJ25" method [5]. The author approximated SRA levels. Because of this layer, the blockchain is protected [6]. Using four different security measures, they handled the vulnerability and analyzed the key's one-of-a-kind qualities [7]. The seven-stage security method used by RPBB31 was investigated by Batcha, B.B.C., in collaboration with other experts [8]. The public mode prompted them to study data interchange and assist with the voting process. This method was used to send data into the blockchain. The author investigated layers of security protocols. Evaluating performance effectiveness may be done in various ways [10]. In order to ensure rapid security, they developed the blockchain hyperledger and responded rapidly. Security is implemented through the use of this feature [11]. A comparison was made between the features of the Internet of Things and blockchain by the author [12]. The majority of their focus is on acquiring security knowledge. The use of federated learning makes security better [13]. The author made a deep learning safety proposal and analysed many blockchain data safety activities [14]. As part of their research, C. B. Basha and colleagues looked at ways to enhance performance and safety [13]. After examining the existing body of scholarship, the RajaprakashBagathbasha-24 (RPBB-24-1) methodology was established. They investigate the reencryption of data stored on IoT blockchains. This process for re-encryption demonstrates that the data is secure [16]. Throughout their discussion, C. Bagath Basha and colleagues offered RPBB-24-1 to make encryption more secure. This method offered a high-level encryption protection that was quick and efficient [17]. After thoroughly examining the suitable approach, we will provide you with the RajaprakashBagathbasha-24-6 (RPBB-24-6) method.

3. Methodology

An RPBB24-6 encryption and decryption process is the way that has been offered, and this method comes with four different processes. Developing a covert message is the first step in the procedure. In the second step of the procedure, you will apply the secret code to each letter of the first secret message and then multiply the code by four times for each letter. Using the matrix as the third procedure, the encrypted data are applied. The application of the salsa approach constitutes the fourth step. Lastly, the plain text has been transformed into well-secured data, as seen in Figure 2.

3.1. Encryption Algorithm

1. To begin, we need to choose secret messages or PT.
2. The secret message is converted to the numbers from the "Latin alphabet" for PT, and each letter is multiplied four times to encrypt the FET.

$$if\ a < n\ Then$$
$$T_a - GT_n$$
$$T_{a\,b} = T_{a\,b} *\ \ T_{a\,b} = R_a * \qquad -(1)$$
$$T_{a\,b} = (R_a *) * T_{a\,b} = R_a *$$
$$T_{a\,b} = (R_a *) * T_{a\,b} = R_a *$$
$$T_{a\,b} = (R_i *) * T_{i\,j} = R_i *$$
$$Where\ T\ is\ Character\ and\ R\ is\ Remainder$$
$$a = 0, a\ =\ a + 1\ to\ n, b = b + 1, b = 0$$
$$and\ n =\ number\ of\ charaters$$
$$else$$
$$a > n\ then\ Stop\ a$$

3. In order to swap the values, the initial encrypted text values in the matrix PT must be applied.
4. Apply the Salsa method to encrypt the SET.

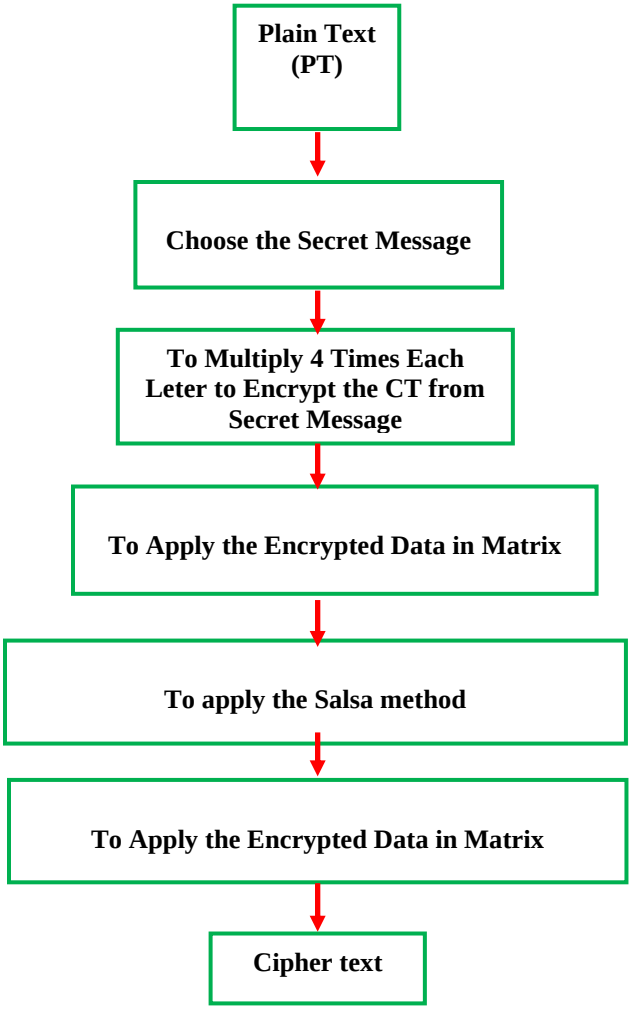

Fig. 3 RPBB-24-6 Methodology

3.2. Decryption Algorithm

1. In order to multiply the DDT matrix, the Salsa method must be applied.
2. Second, we are required to receive a cypher text message from the user as a DDT.
3. The decryption process begins by converting the secret message to the numbers from the "Latin alphabet" for the DDT and multiplying each letter by four to encrypt the FDT.

$$if\ a\ <\ n\ Then$$
$$T_a - GT_n$$
$$T_{a\,b} = T_{a\,b} *\ \ T_{a\,b} = R_a * \quad (2)$$
$$T_{a\,b} = (R_a *) * T_{a\,b} = R_a *$$
$$T_{a\,b} = (R_a *) * T_{a\,b} = R_a *$$
$$T_{a\,b} = (R_i *) * T_{i\,j} = R_i *$$
$$Where\ T\ is\ Character\ and\ R\ is\ Remainder$$
$$a = 0, a\ =\ a + 1\ to\ n, b = b + 1, b = 0$$
$$and\ n =\ number\ of\ charaters$$
$$else$$
$$a > n\ then\ Stop\ a$$

4. In order to swap the values, the first decrypted text values in the matrix DDT must be applied.

4. Result & Discussion

$$PT=\begin{bmatrix} TP_{11} & TP_{12} & TP_{13} & TP_{14} \\ TP_{21} & TP_{22} & TP_{23} & TP_{24} \\ TP_{31} & TP_{32} & TP_{33} & TP_{34} \\ TP_{41} & TP_{42} & TP_{43} & TP_{44} \end{bmatrix}$$

4.1. Working for Encryption

- To choose the secret key as PT
- The first secret key is “GOLD”.
- PT=GOLD
- $G - 71, O - 79, L - 76, D - 68$

$$PT = 71797668$$

- Apply the equation 1 [14].

4.1.1. First Character -G= 71

- $a = 1, b = 1$

$$T_{11} = PT_4$$
$$G - 71, b = 1$$
$$T_{11} = 71 * 71$$
$$T_{11} = 5041/91 \Rightarrow 36b = 2$$
$$T_{12} = 36 * 71$$
$$T_{12} = 2556/91 \Rightarrow 8$$
$$b = 3$$
$$T_{13} = 8 * 71$$
$$T_{13} = 568/91 \Rightarrow 22$$
$$a = 4$$
$$T_{14} = 22 * 71$$
$$T_{14} = 1562/91 \Rightarrow 15$$
$$T_{14} = 15$$

4.1.2. Second Character - O= 79

- $a = a + 1,$

$$a = 1 + 1 = 2$$
$$a = 2, b = 1$$
$$T_{21} = PT_4$$
$$O = 79, b = 1$$
$$T_{21} = 79 * 79$$
$$T_{21} = 6241/91 \Rightarrow 53b = 2$$
$$T_{22} = 53 * 79$$
$$T_{22} = 4187/91 \Rightarrow 1$$
$$b = 3$$
$$T_{23} = 1 * 79$$
$$T_{23} = 79/91 \Rightarrow 79$$
$$b = 4$$
$$T_{24} = 79 * 79$$
$$T_{24} = 6241/91 \Rightarrow 53$$
$$T_{24} = 53$$

4.1.3. Third Character - L= 76

- $a = a + 1,$

$$a = 2 + 1 = 3$$
$$a = 3, b = 1$$
$$T_{31} = PT_4$$
$$L = 76, b = 1$$
$$T_{31} = 76 * 76$$
$$T_{31} = 5776/91 \Rightarrow 43b = 2$$
$$T_{32} = 43 * 76$$
$$T_{32} = 3268/91 \Rightarrow 83$$
$$b = 3$$
$$T_{33} = 83 * 76$$
$$T_{33} = 6308/91 \Rightarrow 29$$
$$b = 4$$
$$T_{34} = 29 * 76$$
$$T_{34} = 2204/91 \Rightarrow 20$$
$$T_{34} = 20$$

4.1.4. Fourth Character - D= 68

- $a = a + 1$

$$a = 3 + 1 = 4$$
$$a = 4, b = 1$$
$$T_{41} = PT_4$$
$$T = 68, b = 1$$
$$T_{41} = 68 * 68$$
$$T_{41} = 4624/91 \Rightarrow 74b = 2$$
$$T_{42} = 74 * 68$$
$$T_{42} = 5032/91 \Rightarrow 27$$
$$b = 3$$
$$T_{43} = 27 * 68$$
$$T_{43} = 1836/91 \Rightarrow 16$$
$$b = 4$$
$$T_{44} = 16 * 68$$
$$T_{44} = 1088/91 \Rightarrow 87$$
$$T_{44} = 87$$

- FET=15532087
- To make a pair, apply the first encrypted text (FET) in the matrix.
- FET=(1,5), (5,3), (2,0), (8,7)

$$PT=\begin{bmatrix} TP_{11} & TP_{12} & TP_{13} & TP_{14} \\ TP_{21} & TP_{22} & TP_{23} & TP_{24} \\ TP_{31} & TP_{32} & TP_{33} & TP_{34} \\ TP_{41} & TP_{42} & TP_{43} & TP_{44} \end{bmatrix}$$

- First swap values (1,5)

$$FET=\begin{bmatrix} TP_{11} & TP_{22} & TP_{13} & TP_{14} \\ TP_{21} & TP_{12} & TP_{23} & TP_{24} \\ TP_{31} & TP_{32} & TP_{33} & TP_{34} \\ TP_{41} & TP_{42} & TP_{43} & TP_{44} \end{bmatrix}$$

- Second swap values (5, 3)

$$FET=\begin{bmatrix} TP_{11} & TP_{22} & TP_{13} & TP_{12} \\ TP_{21} & TP_{14} & TP_{23} & TP_{24} \\ TP_{31} & TP_{32} & TP_{33} & TP_{34} \\ TP_{41} & TP_{42} & TP_{43} & TP_{44} \end{bmatrix}$$

- Third swap values (2, 0)

$$FET=\begin{bmatrix} TP_{13} & TP_{22} & TP_{11} & TP_{12} \\ TP_{21} & TP_{14} & TP_{23} & TP_{24} \\ TP_{31} & TP_{32} & TP_{33} & TP_{34} \\ TP_{41} & TP_{42} & TP_{43} & TP_{44} \end{bmatrix}$$

- Fourth swap values (8, 7)

$$FET=\begin{bmatrix} TP_{13} & TP_{22} & TP_{11} & TP_{12} \\ TP_{21} & TP_{14} & TP_{23} & TP_{31} \\ TP_{24} & TP_{32} & TP_{33} & TP_{34} \\ TP_{41} & TP_{42} & TP_{43} & TP_{44} \end{bmatrix}$$

- To apply the Salsa method in ST (“Salsa Text”)

$$ST=\begin{bmatrix} TP_{13} & TP_{14} & TP_{33} & TP_{44} \\ TP_{21} & TP_{32} & TP_{43} & TP_{12} \\ TP_{24} & TP_{42} & TP_{11} & TP_{31} \\ TP_{41} & TP_{22} & TP_{23} & TP_{34} \end{bmatrix}$$

4.2. Working for Decryption

$$\text{FDT (First Decrypted Text)}=\begin{bmatrix} TP_{13} & TP_{14} & TP_{33} & TP_{44} \\ TP_{21} & TP_{32} & TP_{43} & TP_{12} \\ TP_{24} & TP_{42} & TP_{11} & TP_{31} \\ TP_{41} & TP_{22} & TP_{23} & TP_{34} \end{bmatrix}$$

- Now to apply the Salsa method in FDT

$$FDT=\begin{bmatrix} TP_{13} & TP_{22} & TP_{11} & TP_{12} \\ TP_{21} & TP_{14} & TP_{23} & TP_{31} \\ TP_{24} & TP_{32} & TP_{33} & TP_{34} \\ TP_{41} & TP_{42} & TP_{43} & TP_{44} \end{bmatrix}$$

- SDT=DLOG
- $D-68, L-76, O-79, G-71$

$$SDT = 68767971$$

- Apply the equation 2 [14].

4.2.1. First Character - D= 68

- $a = 1, b = 1$

$$T_{11} = PT_4$$
$$T = 68, b = 1$$
$$T_{11} = 68 * 68$$
$$T_{11} = 4624/91 \Rightarrow 74b = 2$$
$$T_{12} = 74 * 68$$
$$T_{12} = 5032/91 \Rightarrow 27$$
$$b = 3$$
$$T_{13} = 27 * 68$$
$$T_{13} = 1836/91 \Rightarrow 16$$
$$b = 4$$
$$T_{14} = 16 * 68$$
$$T_{14} = 1088/91 \Rightarrow 87$$
$$T_{14} = 87$$

4.2.2. Second Character - L= 76

- $a = a + 1,$

$$a = 1 + 1 = 2$$
$$a = 2, b = 1$$
$$T_{21} = PT_4$$
$$L = 76, b = 1$$
$$T_{21} = 76 * 76$$
$$T_{21} = 5776/91 \Rightarrow 43b = 2$$
$$T_{22} = 43 * 76$$
$$T_{22} = 3268/91 \Rightarrow 83$$
$$b = 3$$
$$T_{23} = 83 * 76$$
$$T_{23} = 6308/91 \Rightarrow 29$$
$$b = 4$$
$$T_{24} = 29 * 76$$
$$T_{24} = 2204/91 \Rightarrow 20$$
$$T_{24} = 20$$

4.2.3. Third Character - O= 79

- $a = a + 1,$

$$a = 2 + 1 = 3$$
$$a = 3, b = 1$$
$$T_{31} = PT_4$$
$$O = 79, b = 1$$
$$T_{31} = 79 * 79$$
$$T_{31} = 6241/91 \Rightarrow 53b = 2$$
$$T_{32} = 53 * 79$$
$$T_{32} = 4187/91 \Rightarrow 1$$
$$b = 3$$
$$T_{33} = 1 * 79$$
$$T_{33} = 79/91 \Rightarrow 79$$
$$b = 4$$
$$T_{34} = 79 * 79$$
$$T_{34} = 6241/91 \Rightarrow 53$$
$$T_{34} = 53$$

4.2.4. Fourth Character -G= 71

- $a = a + 1$

$$a = 3 + 1 = 4$$

$a = 4, b = 1$
$T_{41} = PT_4$
$G - 71, b = 1$
$T_{41} = 71 * 71$
$T_{41} = 5041/91 \Rightarrow 36b = 2$
$T_{42} = 36 * 71$
$T_{42} = 2556/91 \Rightarrow 8$
$b = 3$
$T_{43} = 8 * 71$
$T_{43} = 568/91 \Rightarrow 22$
$a = 4$
$T_{44} = 22 * 71$
$T_{44} = 1562/91 \Rightarrow 15$
$T_{44} = 15$

- SDT=87205315
- To make a pair, apply the second decrypted text (SDT) in the matrix.
- SDT=(8,7), (2,0), (5,3), (1,5)

- First swap values (8,7)

$$SDT=\begin{bmatrix} TP_{13} & TP_{22} & TP_{11} & TP_{12} \\ TP_{21} & TP_{14} & TP_{23} & TP_{24} \\ TP_{31} & TP_{32} & TP_{33} & TP_{34} \\ TP_{41} & TP_{42} & TP_{43} & TP_{44} \end{bmatrix}$$

- Second swap values (2, 0)

$$SDT=\begin{bmatrix} TP_{11} & TP_{22} & TP_{13} & TP_{12} \\ TP_{21} & TP_{14} & TP_{23} & TP_{24} \\ TP_{31} & TP_{32} & TP_{33} & TP_{34} \\ TP_{41} & TP_{42} & TP_{43} & TP_{44} \end{bmatrix}$$

- Third swap values (5,3)

$$SDT=\begin{bmatrix} TP_{11} & TP_{22} & TP_{13} & TP_{14} \\ TP_{21} & TP_{12} & TP_{23} & TP_{24} \\ TP_{31} & TP_{32} & TP_{33} & TP_{34} \\ TP_{41} & TP_{42} & TP_{43} & TP_{44} \end{bmatrix}$$

- Fourth swap values (1, 5)

$$SDT=\begin{bmatrix} TP_{11} & TP_{12} & TP_{13} & TP_{14} \\ TP_{21} & TP_{22} & TP_{23} & TP_{24} \\ TP_{31} & TP_{32} & TP_{33} & TP_{34} \\ TP_{41} & TP_{42} & TP_{43} & TP_{44} \end{bmatrix}$$

A comparison of the two different encryption speeds is shown in Table 1, which may be accessed at this location. Compared to other methods that are now in use, it has been noted that the one-of-a-kind strategy known as RPBB-24-6 possesses greater performance in terms of speed. In various file sizes, the novel approach RPBB-24-6 shows performance speeds of 2.5, 2.9, 3.3, 3.6, 4.1, 4.6, and 5.1. These speeds are measured in milliseconds. In addition, the unique approach has great performance compared to existing methods, such as the "Salsa" method shown in Figure 4, RBJ25 in Figure 5, and the new method in Figure 6.

Table 1. RPBB-24-6 Encryption performance

File Size (Bytes)	Salsa	RBJ25	RPBB-24-6
25	1.69	2.2	2.5
77	1.29	2.6	2.9
110	1.09	2.8	3.3
311	2.73	3.1	3.6
811	2.64	3.8	4.1
1521	3.4	4.2	4.6
6580	2.27	4.6	5.1

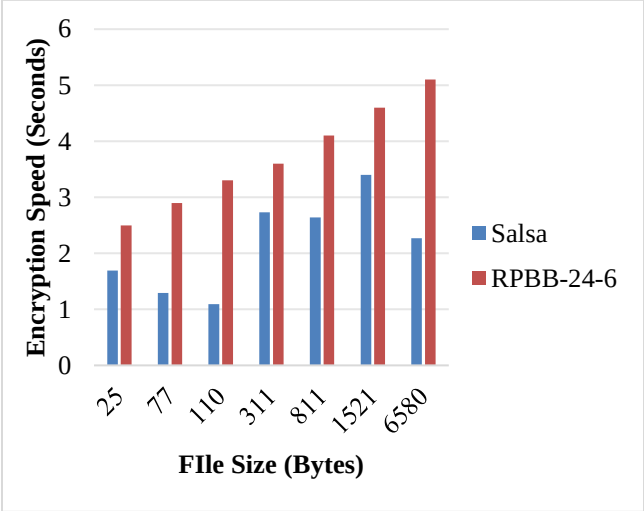

Fig. 4 Salsa vs RPBB-24-6 Encryption speed

According to Table 2, the performance of the three different decryption speeds is shown. A comparison of the unique approach Double RPBB-24-6 with existing methods reveals that it demonstrates superior performance in terms of speed. The performance speed for the unique technique RPBB-24-6 is 2.5, 2.9, 3.6, 3.9, 4.5, 4.9, and 5.1 in various file sizes. Additionally, the method has a strong performance compared to existing methods, such as the "Salsa" method shown in Figure 7, RBJ25 in Figure 8, and the new method in Figure 9.

Table 2. RPBB-24-6 Decryption performance

File Size (Bytes)	Salsa	RBJ25	RPBB-24-6
25	1.3	1.9	2.5
77	1.6	2.3	2.9
110	2.1	2.8	3.6
311	2.6	3.5	3.9
811	2.8	4.1	4.5
1521	3.1	4.5	4.9
6580	3.3	4.8	5.1

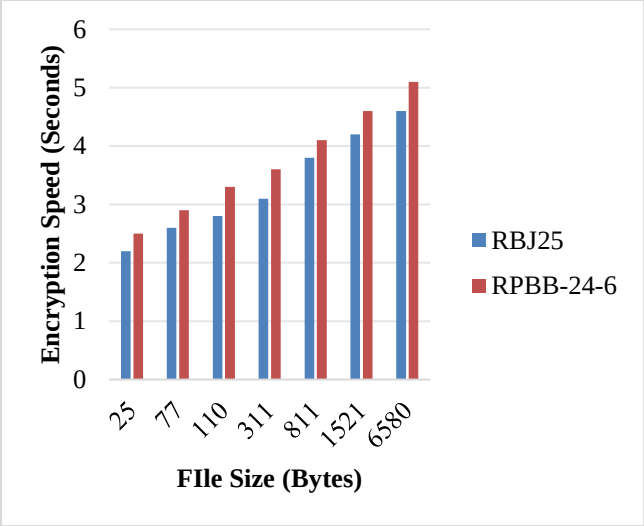

Fig. 5 RBJ25 Vs RPBB-24-6 Encryption speed

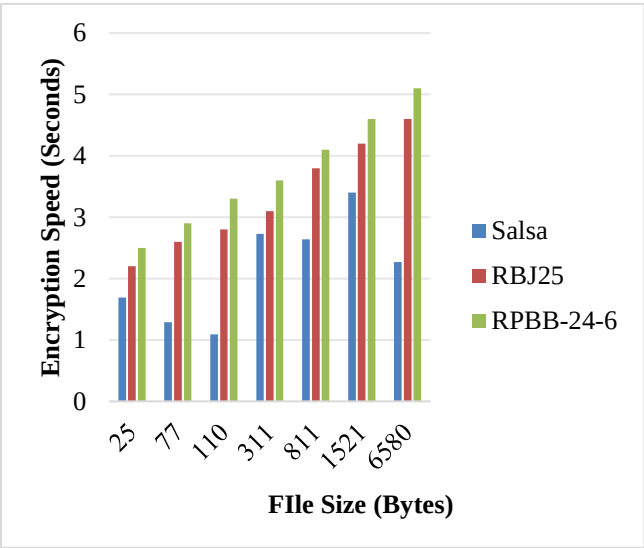

Fig. 6 Salsa Vs RBJ25 Vs RPBB-24-6 Encryption speed

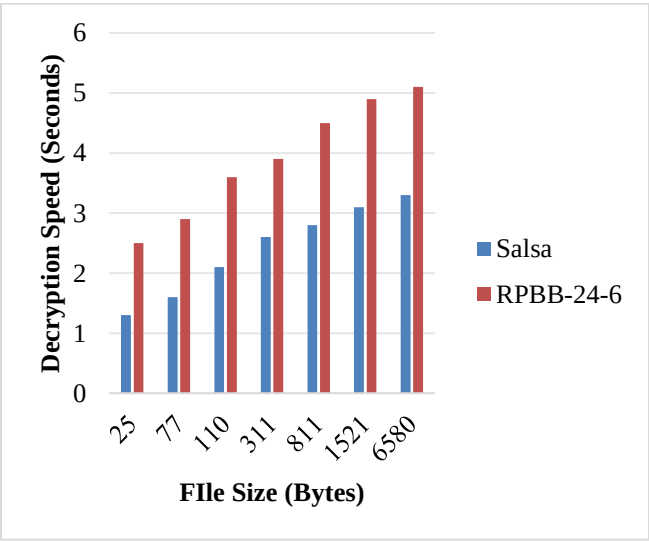

Fig. 7 Salsa Vs RPBB-24-6 Decryption speed

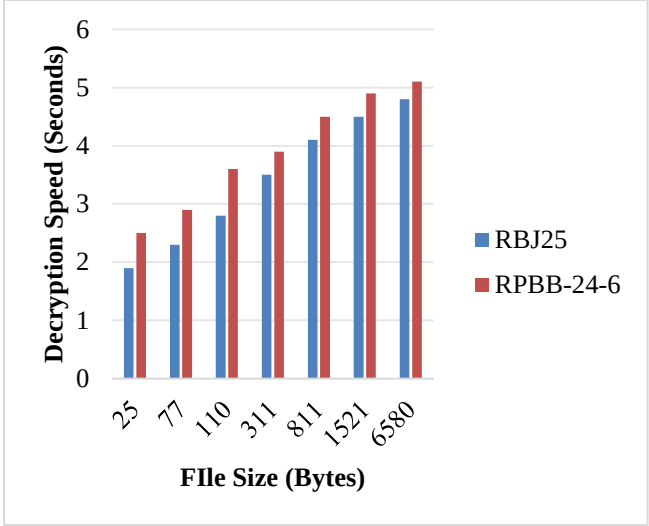

Fig. 8 RBJ25 Vs RPBB-24-6 Decryption speed

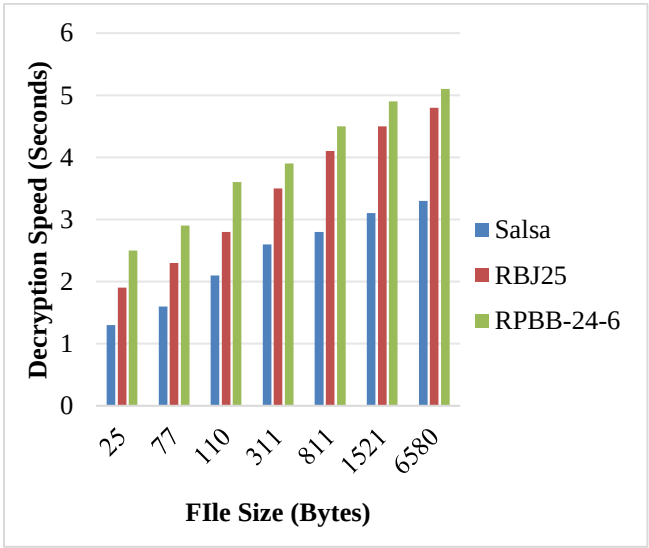

Fig. 9 Salsa Vs RBJ25 Vs RPBB-24-6 Decryption Speed

5. Conclusion

Blockchain technology is one of the emerging platforms that is seeing the most rapid expansion globally. Although many people have never heard of it, Block Chain is a technology used to safeguard various types of data. These folks continue to use the “Salsa” software, which is less secure. This document proposes a method of safeguarding items referred to as RPBB-24-6. An encryption and decoding procedure based on RPBB24-6 has been proposed as a potential alternative measure. This method has four different steps. The first step of the process is to develop a secret message. You will apply the secret code to each letter of the first secret message and then increase the code by four for each letter in the second step. The protected data are used in the third step, the grid. Fourth, the salsa method needs to be put into practice. After a long time, the plain text was finally turned into safe data.

References

[1] Muhammad Nasir Mumtaz Bhutta et al., "A Survey on Blockchain Technology: Evolution, Architecture and Security," *IEEE Access*, vol. 9, pp. 61048-61073, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[2] Suhyeon Lee, and Seungjoo Kim, "Blockchain as a Cyber Defense: Opportunities, Applications, and Challenges," *IEEE Access*, vol. 10, pp. 2602-2618, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[3] Mohammad Wazid, Ashok Kumar Das, and Youngho Park, "Generic Quantum Blockchain-Envisioned Security Framework for IoT Environment: Architecture, Security Benefits and Future Research," *IEEE Open Journal of the Computer Society*, vol. 5, pp. 248-267, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[4] Mubashar Iqbal, and Raimundas Matulevicius, "Exploring Sybil and Double-Spending Risks in Blockchain Systems," *IEEE Access*, vol. 9, pp. 76153-76177, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[5] S. Rajaprakash et al., "RBJ25 Cryptography Algorithm for Securing Big Data," *Journal of Physics: Conference Series*, vol. 1706, pp. 1-8, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[6] Ivan Homoliak et al., "The Security Reference Architecture for Blockchains: Toward a Standardized Model for Studying Vulnerabilities, Threats, and Defenses," *IEEE Communications Surveys and Tutorials*, vol. 23, no. 1, pp. 341-390, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[7] Yongfeng Huang et al., "Smart Contract Security: A Software Lifecycle Perspective," *IEEE Access*, vol. 7, pp. 150184-150202, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[8] Bagath Basha Chan Batcha, et al., "A Novel Security Algorithm RPBB31 for Securing the Social Media Analyzed Data using Machine Learning Algorithms," *Wireless Personal Communications*, vol. 131, pp. 581-608, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[9] Weiqi Dai et al., "PRBFPT: A Practical Redactable Blockchain Framework with a Public Trapdoor," *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 2425-2437, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[10] Yong Wang et al., "Cloud-Assisted EHR Sharing with Security and Privacy Preservation Via Consortium Blockchain," *IEEE Access*, vol. 7, pp. 136704-136719, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[11] Zeeshan Zulkifl et al., "FBASHI: Fuzzy and Blockchain-Based Adaptive Security for Healthcare IoTs," *IEEE Access*, vol. 10, pp. 15644-15656, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[12] Nathalie Tan Yhe Huan, and Zuriati Ahmad Zukarnain, "A Survey on Addressing IoT Security Issues by Embedding Blockchain Technology Solutions: Review, Attacks, Current Trends, and Applications," *IEEE Access*, vol. 12, pp. 69765-69782, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[13] C. Bagath Basha et al., "An Innovative Cryptography Safety Algorithm Called S-RSB-23 for Protecting Data Using Machine Learning Algorithm," *International Journal of Intelligent Systems and Applications in Engineering*, vol. 12, no. 2S, pp. 503-510, 2024. [Publisher Link]

[14] Oumaima Fadi et al., "A Survey on Blockchain and Artificial Intelligence Technologies for Enhancing Security and Privacy in Smart Environments," *IEEE Access*, vol. 10, pp. 93168-93186, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[15] Shailendra Rathore, Jong Hyuk Park, and Hangbae Chang, "Deep Learning and Blockchain-Empowered Security Framework for Intelligent 5G-Enabled IoT," *IEEE Access*, vol. 9, pp. 90075-90083, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[16] Kwame Opuni-Boachie Obour Agyekum et al., "A Proxy Re-Encryption Approach to Secure Data Sharing in the Internet of Things Based on Blockchain," *IEEE Systems Journal*, vol. 16, no. 1, pp. 1685-1696, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[17] C. Bagath Basha et al., "The Design of Security Algorithm RPBB-24-1 in Multi-Way Path over the Distributed Ledger," *International Journal of Electrical and Electronics Engineering*, vol. 11, no. 4, pp. 36-44, 2024. [CrossRef] [Google Scholar] [Publisher Link]